www.coe.int/cybercrime

Strasbourg, le 27 juin 2023 T-CY(2023)6

Comité de la Convention sur la Cybercriminalité (T-CY)

Note d'orientation n° 13 du T-CY
La portée d'application des pouvoirs de procédure et des dispositions portant sur la coopération internationale de la Convention de Budapest

Adoptée par le T-CY
lors de sa 28e réunion plénière (27-28 juin 2023)

Contact

Alexander Seger

Secrétaire exécutif du Comité de la Convention sur la Cybercriminalité
Direction générale des droits de l'homme et de l'État de droit
Conseil de l'Europe, Strasbourg, France

Tél. +33-3-9021-4506
Fax +33-3-9021-5650
Courriel alexander.seger@coe.int

1 Introduction

Lors de sa 8e session plénière (décembre 2012), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, y compris à la lumière des nouveautés juridiques, politiques ou techniques[1]. Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note concerne la portée d'application des pouvoirs de procédure au niveau national et des dispositions portant sur la coopération internationale de la Convention sur la cybercriminalité (STE nº 185) et de son Deuxième Protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE nº 224).

Si le texte de la Convention sur la cybercriminalité indique clairement que les pouvoirs procéduraux et les dispositions relatives à la coopération internationale sont applicables non seulement à la cybercriminalité (articles 2 à 11 de la Convention), mais aussi « à toutes les autres infractions pénales commises au moyen d'un système informatique » et « à la collecte des preuves électroniques de toute infraction pénale » (article 14.2 b et c ; et articles 23 et 25 de la STE nº 185), et bien que cela soit confirmé par le Deuxième Protocole additionnel à la Convention (article 2 de la STCE nº 224), ce champ d'application n'est pas toujours bien compris et certaines législations nationales limitent l'application des pouvoirs de procédure ou des dispositions relatives à la coopération internationale à un ensemble de cybercrimes.

Le T-CY a donc estimé que la rédaction d'une note d'orientation précisant comment les principales dispositions en matière de procédure et de coopération internationale pourraient s'appliquer non seulement aux infractions commises contre et au moyen de systèmes informatiques, mais aussi à toute une série d'infractions, présentait un intérêt pratique et stratégique.

2 Dispositions pertinentes de la Convention sur la cybercriminalité (STE nº 185)

2.1 Dispositions procédurales

En vertu de la Convention sur la cybercriminalité, « [c]haque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes de » prendre les mesures procédurales énoncées aux articles 16 à 21 de la Convention :

- Article 16 – Conservation rapide de données informatiques stockées
- Article 17 – Conservation et divulgation rapides de données relatives au trafic
- Article 18 – Injonction de produire
- Article 19 – Perquisition et saisie de données informatiques stockées
- Article 20 – Collecte en temps réel des données relatives au trafic
- Article 21 – Interception de données relatives au contenu

Ces mesures sont soumises aux conditions et sauvegardes prévues à l'article 15.

La portée d'application de ces mesures procédurales est définie à l'article 14 :

> Article 14 – Portée d'application des mesures du droit de procédure

[1] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :
   a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;
   b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et
   c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.
   b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services :
      i. qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
      ii. qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

   cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Conformément à l'article 14.2 de la Convention, les pouvoirs de procédure sont donc applicables à la collecte de preuves sous forme électronique de toute infraction pénale. De la sorte, « les preuves électroniques de toute infraction pénale peuvent être obtenues ou collectées au moyen des pouvoirs et des procédures énoncés dans [cette] section » de la Convention (paragraphe 141 du rapport explicatif de la Convention).

Le paragraphe 3 de l'article 14 prévoit des exceptions à ce vaste champ d'application et permet aux Parties de restreindre la portée des pouvoirs plus inclusifs (comme la collecte en temps réel des données relatives au trafic (article 20) ou l'interception de données relatives au contenu (article 21)).[2]

En conséquence, les autorités compétentes peuvent ordonner la conservation de données, ordonner la production de données, perquisitionner ou saisir des données informatiques stockées, ou ordonner ou effectuer la collecte en temps réel de données relatives au trafic ou l'interception

[2] Voir les réserves et déclarations des Parties concernant l'article 14.

de données relatives au contenu[3] dans le cadre d'enquêtes pénales spécifiques liées à toute infraction prévue par le droit national, y compris par exemple[4] :

- la corruption ;
- la contrefaçon de médicaments ou d'autres infractions menaçant la santé publique, y compris les infractions liées à la COVID-19 ;
- les différentes formes de maltraitance des enfants ;
- les différentes formes de violence familiale et de violence à l'égard des femmes ;
- les différentes formes d'infractions économiques et financières ;
- les infractions liées à la drogue ;
- la fraude ;
- les enlèvements ;
- la manipulation de compétitions sportives ;
- le blanchiment de capitaux et le financement du terrorisme ;
- les meurtres ;
- les infractions ayant trait au crime organisé ;
- les viols et autres formes de violence sexuelle ;
- le terrorisme ;
- les génocides, crimes contre l'humanité, crimes de guerre et autres crimes internationaux ;
- la traite des êtres humains ;
- la xénophobie, le racisme et d'autres formes de discours de haine.

2.2 Dispositions relatives à la coopération internationale

Le vaste champ d'application des pouvoirs procéduraux au niveau national s'étend aux principes et aux mesures liés à la coopération internationale (chapitre III de la Convention). Les articles 23 et 25 énoncent clairement que la coopération est non seulement possible aux fins d'investigation ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques, mais aussi pour la collecte de preuves sous forme électronique de toute infraction pénale :

> Article 23 – Principes généraux relatifs à la coopération internationale
>
> Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.
>
> Article 25 – Principes généraux relatifs à l'entraide
>
> 1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données

[3] Comme indiqué aux articles 20 et 21 de la Convention, la collecte en temps réel de données relatives au trafic et l'interception de données relatives au contenu peuvent faire l'objet de certaines restrictions, telles que la limitation imposée aux infractions graves.

[4] Voir également ci-dessous les références aux traités internationaux pertinents pour certaines de ces infractions.

informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Le paragraphe 243 du rapport explicatif de la Convention confirme par ailleurs :

> « la coopération doit s'étendre à toutes les infractions pénales liées à des systèmes et données informatiques (c'est-à-dire les infractions visées par l'article 14, paragraphe 2, lettres a et b), ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale. En d'autres termes, les clauses du chapitre III sont applicables soit aux situations où l'infraction est commise à l'aide d'un système informatique, soit à celles où une infraction ordinaire, non commise à l'aide d'un système informatique (par exemple un meurtre), donne lieu à la collecte de preuves sous forme électronique. »

Les Parties peuvent restreindre ce vaste champ d'application en ce qui concerne l'entraide dans la collecte en temps réel de données relatives au trafic (article 33) et l'entraide en matière d'interception de données relatives au contenu (article 34). En outre, la coopération internationale peut être subordonnée à certaines conditions, comme l'existence d'une double incrimination[5] ou les motifs de refus prévus aux articles 25.4, 27.4 et 27.5[6] de la Convention.

Les principes et mesures de coopération internationale concernant les infractions énumérées dans la Convention et les autres infractions pénales commises au moyen d'un système informatique, ainsi que la collecte de preuves électroniques de toute autre infraction pénale, sont énoncés aux articles 23 à 35[7] de la Convention :

- Article 23 – Principes généraux relatifs à la coopération internationale ;
- Article 25 – Principes généraux relatifs à l'entraide ;
- Article 26 – Information spontanée ;
- Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables ;
- Article 28 – Confidentialité et restriction d'utilisation ;
- Article 29 – Conservation rapide de données informatiques stockées ;
- Article 30 – Divulgation rapide de données conservées ;
- Article 31 – Entraide concernant l'accès aux données stockées ;
- Article 32 – Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public ;
- Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic ;
- Article 34 – Entraide en matière d'interception de données relatives au contenu ;
- Article 35 – Réseau 24/7.

Les Parties à la Convention peuvent recourir à ces mesures et principes pour coopérer entre elles dans toute la mesure possible aux fins d'investigations ou de procédures et de collecte de preuves sous forme électronique de toute infraction pénale, et demander la conservation des données,

---

[5] Voir l'article 29.4 de la Convention.
Comme l'énonce le paragraphe 259 du rapport explicatif de la Convention, « [d]ans les affaires auxquelles le critère de la double incrimination est applicable, il devrait l'être d'une façon souple, de nature à faciliter l'octroi de l'assistance ».

[6] L'article 27.5 de la Convention se réfère aux motifs d'ajournement d'une action suite à une demande.

[7] Note : l'obligation d'extrader prévue à l'article 24 (Extradition) s'applique uniquement aux « infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère ».

l'accès à des données informatiques stockées, la collecte en temps réel de données relatives au trafic ou l'interception de données relatives au contenu[8], ou encore l'accès transfrontalier à des données informatiques stockées avec le consentement de l'intéressé ou lorsqu'elles sont accessibles au public, en ce qui concerne toute infraction pénale et dans les conditions prévues au chapitre III de la Convention.

3 Dispositions pertinentes du Deuxième Protocole additionnel (STCE n° 224)

Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE n° 224) a été ouvert à la signature le 12 mai 2022. Après son entrée en vigueur, cet instrument offrira aux Parties des outils supplémentaires pour « renforcer la coopération et la divulgation des preuves électroniques ».

Ce protocole a lui aussi un vaste champ d'application et s'applique non seulement aux infractions pénales liées aux systèmes et aux données informatiques, mais également à la collecte de preuves sous forme électronique de toute infraction pénale :

> Article 2 – Champ d'application
>
> 1 Sauf dispositions contraires prévues au présent Protocole, les mesures qu'il énonce s'appliquent :
>
> a pour ce qui concerne les Parties à la Convention qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique ; et
>
> b pour ce qui concerne les Parties au Premier Protocole qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole.

Les mesures prévues par ce Protocole sont les suivantes :

- Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine directement auprès d'une entité fournissant des services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie ;
- Article 7 – Divulgation de données relatives aux abonnés par le biais d'une coopération directe avec un fournisseur situé sur le territoire d'une autre Partie ;
- Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic ;
- Article 9 – Divulgation accélérée de données informatiques stockées en situation d'urgence ;
- Article 10 – Demande d'entraide urgente ;

[8] Comme indiqué aux articles 20 et 21 de la Convention, la collecte en temps réel de données relatives au trafic et l'interception de données relatives au contenu peuvent faire l'objet de certaines restrictions, telles que la limitation imposée aux infractions graves. En ce qui concerne les articles 33 et 34 sur la coopération internationale, « [c]haque partie accorde cette assistance au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne » (article 33.2), et s'agissant de l'interception des données relatives au contenu, « [l]es Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables […] » (article 34).

– Article 11 – Vidéoconférence ;
– Article 12 – Équipes communes d'enquête et enquêtes communes.

Ces mesures sont soumises aux conditions et sauvegardes prévues aux articles 13 et 14 de la STCE n° 224.

Par conséquent, les autorités compétentes des parties au présent protocole peuvent, en tenant compte des réserves et des déclarations autorisées par l'article 19 de la STCE n°224, demander des informations sur l'enregistrement des noms de domaine, ordonner la divulgation d'informations relatives aux abonnés, donner suite à des injonctions de production d'informations sur les abonnés et de données relatives au trafic, coopérer en cas d'urgence, recourir à la vidéoconférence ou mettre en place des équipes communes d'enquête ou participer à des enquêtes communes liées à des enquêtes ou à des procédures pénales concernant des infractions pénales en rapport avec des systèmes et des données informatiques ainsi que la collecte de preuves sous forme électronique de toute infraction.

4 Synergies entre la Convention sur la cybercriminalité et d'autres traités

Les pouvoirs procéduraux au niveau national et les principes et mesures de coopération internationale peuvent également être utilisés pour recueillir des preuves électroniques relatives à des infractions prévues par d'autres accords internationaux auxquels les États sont Parties, sous réserve des conditions pertinentes mentionnées plus haut[9]. Ces accords peuvent porter sur la corruption[10] ; la contrefaçon de médicaments ou d'autres infractions menaçant la santé publique[11] ; la maltraitance des enfants[12] ; la violence domestique et la violence à l'égard des femmes[13] ; les infractions liées à la drogue[14] ; la manipulation de compétitions sportives[15] ; le blanchiment de capitaux et le financement du terrorisme[16] ; les infractions liées à la criminalité

[9] Telles que l'existence d'une double incrimination ou les motifs de refus prévus aux articles 25.4 et 27.4 de la Convention.

[10] Par exemple, les actes criminels couverts par la Convention pénal sur la corruption (ETS 173) du Conseil de l'Europe ou la Convention des Nations Unies contre la corruption.

[11] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe sur la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique (STCE n° 211).

[12] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).

[13] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE n° 210).

[14] Par exemple, les actes criminels couverts par les Conventions Internationales sur le Contrôle des Drogues.

[15] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe sur la manipulation de compétitions sportives (STCE n° 215).

[16] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n° 198).

organisée[17] ; le terrorisme[18] ; la traite des êtres humains[19] ; ou le génocide, les crimes contre l'humanité, les crimes de guerre et autres crimes internationaux[20].

Pour les Parties au premier Protocole additionnel à la Convention sur la cybercriminalité relatif aux actes de xénophobie et de racisme commis par le biais de systèmes informatiques (STE n° 189)[21], l'article 8.2 indique que les « Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole ».

En 2018, le T-CY a recommandé que les Parties à la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201) et à la Convention d'Istanbul sur la violence contre les femmes et la violence domestique (STCE n° 210) soient encouragées à « introduire dans leur droit interne les pouvoirs procéduraux prévus aux articles 16 à 21 de la Convention de Budapest et de devenir parties à la Convention de Budapest pour faciliter la coopération internationale en matière de preuve électronique (articles 23 à 35 de la Convention de Budapest) en relation avec la violence sexuelle en ligne contre les enfants »[22].

5 Déclaration du T-CY

Le T-CY convient que les dispositions de droit procédural et les principes et mesures de la coopération internationale de la Convention sur la cybercriminalité sont applicables non seulement aux infractions liées aux systèmes et données informatiques, mais aussi à la collecte de preuves électroniques de toute infraction pénale. Ce vaste champ d'application s'applique également aux mesures prévues par le Deuxième Protocole additionnel à la Convention.

Ce champ d'application permet en outre de dégager des synergies entre la Convention de Budapest et d'autres accords internationaux.

---

[17] Par exemple, les actes criminels couverts par la Convention des Nations Unies contre la criminalité transnationale organisées et les protocoles s'y rapportant.

[18] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe pour la prévention du terrorisme (STCE n° 196)et les protocoles s'y rapportant.

[19] Par exemple, les actes criminels couverts par la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains (STCE n° 197).

[20] Par exemple, les actes criminels couverts par la Convention pour la prévention et la répression du crime de génocide de 1948, les quatre Conventions de Genève sur le droit international humanitaire et leurs protocoles additionnels de 1949, ou le Statut de Rome de la Cour pénale internationale.

[21] Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189).

[22] Voir l'étude cartographique du T-CY sur la cyberviolence https://rm.coe.int/t-cy-2017-10-cbg-study-fr-v2/1680993e65